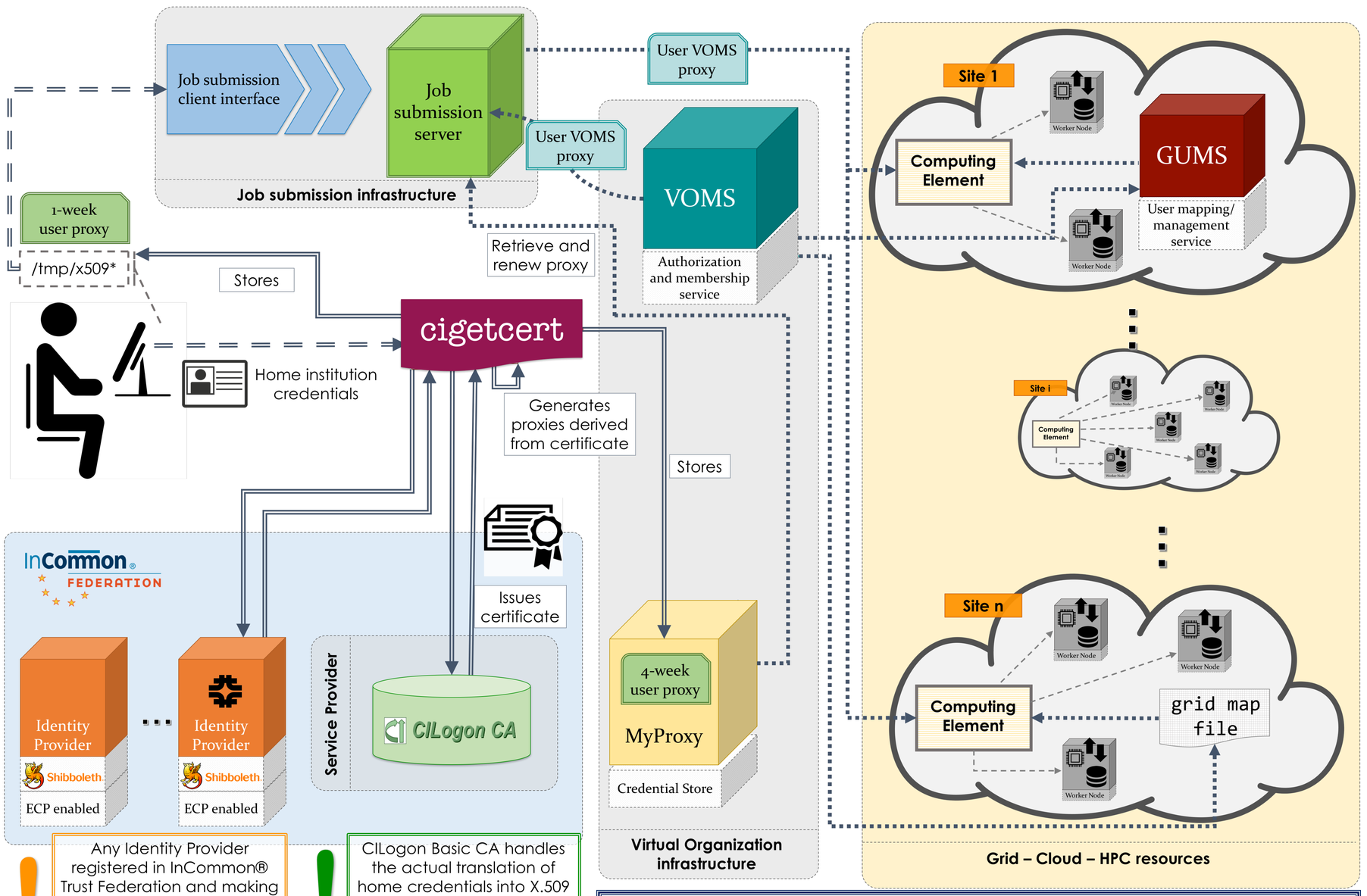
Grid Access with Federated Identities

Dave Dykstra, Mine Altunay, Jeny Teheran, Tanya Levshina,
Neha Sharma, Dennis Box, Kenneth Herner, Amanda Gao.
Scientific Computing Division, Fermilab, Batavia, IL

Key takeaways

- **cigetcert** is an open source, general purpose command line tool developed for this project. It enables federation-based authentication technologies for grid access. Any VO could use this tool to create certificates for their users with logins at institutions in the InCommon® Federation or any other federation supporting a SAML ECP X.509 certificate Service Provider.
- Our system isolates users from the certificate management process. A user only authenticates with his/her home organization in the same manner she/he always does (e.g. username/password or Kerberos). **cigetcert** facilitates this authentication and generates certificates transparent to the user with the help of CILogon Basic CA. The infrastructure manages certificates for the user.
- **cigetcert** stores a proxy certificate on the local disk and stores a longer-lived proxy in **MyProxy** for use by a job submission system to renew authentication so long-lived jobs can access storage.

Architecture



Motivation

- Managing certificates by hand is often an impediment for grid users that are not tech-savvy.
- Fermilab had a grid job management system which managed certificates for users but was completely dependent on Kerberos tickets issued by a Fermilab Kerberos Certifying Authority (KCA).
  - This forced collaborating scientists to create local accounts at Fermilab or learn to configure Fermilab Kerberos authentication on their own machines, both of which proved difficult.
  - The KCA was expensive to maintain and losing software support.

Our goal

- To create a system where non-Fermilab collaborators can access our tools with low barriers using their own home institution credentials.

Status and Future plans

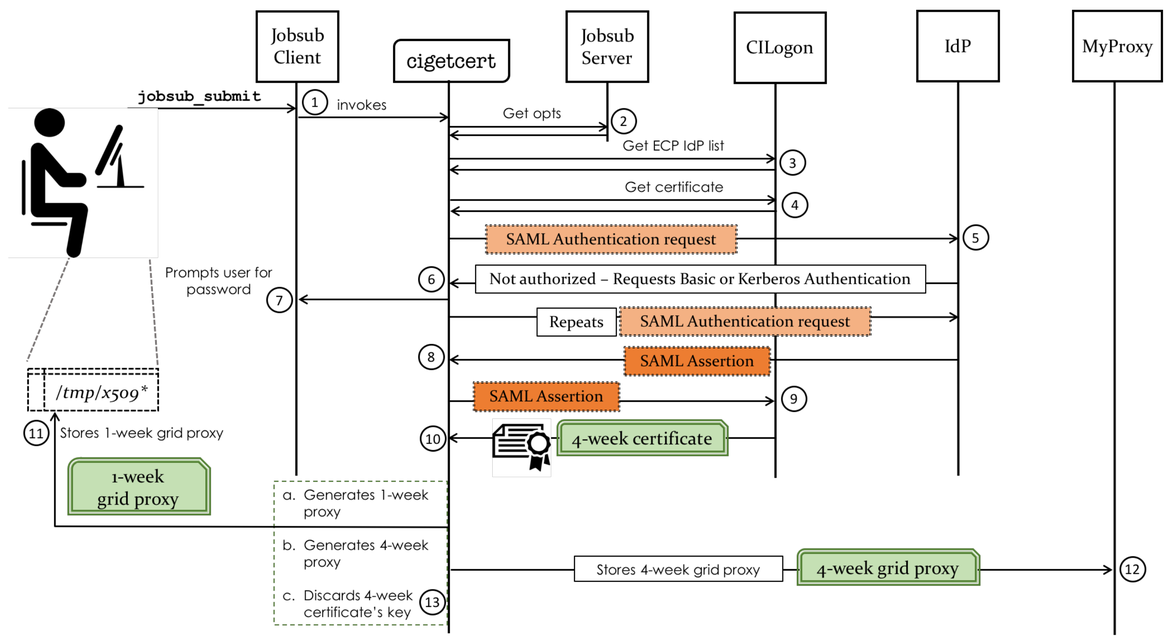
- Phase 1, using only the Fermilab IdP and automatically registering user DNs in VOMS, is complete and in production.
- Phase 2 is scheduled for next year. The goal is to configure **cigetcert** to use other InCommon IdPs and create a new web service with federated single-sign-on to register user DNs automatically in VOMS.
- **cigetcert** is available at https://github.com/fermitools/cigetcert

Work supported by the U.S. Department of Energy under contract No. DE-AC02-07CH11359.

CHEP abstract ID: 183.

Design

- Make use of existing InCommon CILogon Basic CA and existing InCommon federated Identity Providers (IdPs).
  - Enable Enhanced Client or Proxy (ECP) option on the IdPs.
- Write new **cigetcert** command line tool to get certificates on users' behalf:
  - Generic open source tool, not Fermilab-specific.
  - Authenticate users with either Kerberos ticket or username/password.
  - Get 4-week certificate from CILogon Basic CA.
  - Generate and store 1-week proxy on local disk, and 4 week proxy in MyProxy, both unencrypted.
    - Complies with International Grid Trust Foundation (IGTF) rules.
  - Re-use proxy certificates that have enough time remaining, to reduce server load.



- Modify Fermilab job submission system to use **cigetcert** tool:
  - If a Fermilab user already has a Kerberos ticket, use it for authentication. If not, tell user to run **cigetcert** to enter his or her password.
- Modify job submission server to renew user proxies from MyProxy.